

AWS

Screenshot of the AWS IAM Users page showing two users: aws\_user and iam\_user.

**Users (2) Info**

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity	MFA	Password age
aws_user	/	0	15 hours ago	-	19 hours
iam_user	/	0	-	-	7 minutes

**iam\_user Info**

**Summary**

ARN: arn:aws:iam::692859946799:user/iam_user	Console access: Enabled without MFA	Access key 1: Create access key
Created: October 21, 2024, 14:07 (UTC+05:30)	Last console sign-in: Never	

**Permissions**

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly

**Permissions boundary (not set)**

Screenshot of the AWS IAM Users page showing a single user named "aws\_user".

The left sidebar shows the IAM navigation menu with "Users" selected. The main content area displays the "Users (1) Info" section, which includes a search bar and a table with one row:

User name	Path	Groups	Last activity	MFA	Password age	Console access
aws_user	/	0	15 hours ago	-	19 hours	Octob...

At the bottom right of the table are "Edit", "Delete", and "Create user" buttons.

## Console access granted

Screenshot of the AWS IAM User details page for "iam\_user".

The left sidebar shows the IAM navigation menu with "Users" selected. The main content area displays the "iam\_user Info" section, which includes tabs for "Summary", "Permissions", "Groups", "Tags", "Security credentials", and "Last Accessed".

The "Summary" tab shows the following details:

ARN	Console access	Access key 1
arn:aws:iam::692859946799:user/iam_user	Enabled without MFA	Create access key
Created October 21, 2024, 14:07 (UTC+05:30)	Last console sign-in Never	

The "Security credentials" tab shows:

- Console sign-in link: <https://692859946799.signin.aws.amazon.com/console>
- Console password: Updated 9 minutes ago (2024-10-21 14:07 GMT+5:30)
- Last console sign-in: Never

The "Multi-factor authentication (MFA) (0)" section indicates 0 MFA devices assigned.

## Access key generation

The screenshot shows the 'Create access key' wizard on the AWS IAM console. The user has selected the 'Third-party service' option. A warning message at the bottom of the form states: 'As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys.' A checkbox below the message is checked, indicating acceptance of the recommendation.

Local code  
Application running on an AWS compute service  
**Third-party service**  
Application running outside AWS  
Other

**Alternative recommended**  
As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys. [Learn more](#)

Confirmation  
 I understand the above recommendation and want to proceed to create an access key.

Cancel **Next**

The screenshot shows the 'Create access key' wizard on the AWS IAM console, Step 2: Retrieve access keys. It displays the generated access key and secret access key. The access key is AKIA2CUNLY4XXSGURPS2 and the secret access key is YlT7KNyjFn1iTXSUv4zPYKfqNnL0dz0swgmwtNz. A 'Done' button is visible at the bottom right.

Access key created  
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > iam\_user > Create access key

Step 1  
Access key best practices & alternatives

Step 2 - optional  
Set description tag

Step 3  
Retrieve access keys

**Retrieve access keys**

**Access key**  
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIA2CUNLY4XXSGURPS2	YlT7KNyjFn1iTXSUv4zPYKfqNnL0dz0swgmwtNz <a href="#">Hide</a>

**Access key best practices**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file **Done**

## I am user login

AWS exam - Google Doc | Untitled document - Go | **Amazon Web Services S** +

eu-north-1.signin.aws.amazon.com/oauth

Try the new sign in UI  
See our new improved Amazon Web Services sign in experience before we officially launch.

Enable new sign in

**aws**

**Sign in as IAM user**

Account ID (12 digits) or account alias

IAM user name

Password

Remember this account

**Sign in**

[Sign in using root user email](#)  
[Forgot password?](#)

Amazon Lightsail  
Lightsail is the easiest way to get started on AWS

Learn more »

English ▾

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.



## Can access the ec2 instance my the user

The screenshot shows the AWS EC2 Home page in the N. Virginia region. The left sidebar includes sections for EC2 Dashboard, Instances, Images, Elastic Block Store, Network & Security, and CloudShell/Feedback. The main content area displays a summary of resources: 1 Instance (running), 0 Capacity Reservations, 0 Elastic IPs, 1 Key pairs, 0 Placement groups, 0 Snapshots, 0 Auto Scaling Groups, 0 Dedicated Hosts, 1 Instances, 0 Load balancers, 6 Security groups, and 1 Volumes. Below this, there are two main sections: 'Launch instance' (with 'Launch instance' and 'Migrate a server' buttons) and 'Service health' (which shows an error message: 'An error occurred An error occurred retrieving service health information' and a 'Diagnose with Amazon Q' button). On the right side, there's a 'EC2 Free Tier Info' section with a note about IAM user authorization and a link to view global EC2 resources.

## He can create the instance

Screenshot of the AWS CloudShell interface showing the creation of an EC2 instance.

**Network settings:**

- Network: vpc-032188921aaa095d7
- Subnet: No preference (Default subnet in any availability zone)
- Auto-assign public IP: Enable
- Additional charges apply when outside of free tier allowance
- Firewall (security groups):
  - Create security group (selected)
  - Select existing security group
- We'll create a new security group called 'launch-wizard-3' with the following rules:
  - Allow SSH traffic from Anywhere (0.0.0.0/0)
  - Allow HTTPS traffic from the internet
  - Allow HTTP traffic from the internet
- A warning message: Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

**Summary:**

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2... (read more)
- Virtual server type (instance type): t3.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB
- A callout box for the Free tier:
 

In your first year includes

750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 200 MB of S3 storage, and 100 GB of CloudWatch Log storage.

**Actions:**

- Cancel
- Launch Instance
- Preview code

**Instances (2) Info:**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
naya_wala	i-0de10628813f4152c	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1d
user_instance	i-009742ed1bad2478b	Running	t3.micro	Initializing	View alarms +	us-east-1d

**Select an instance:**

## Connect with ssh

AWS exam - Google Doc | Connect to instance | EC2 Instance Connect

us-east-1.console.aws.amazon.com/ec2/home

aws Services Search [Option+S] N. Virginia iam\_user @ 6928-5994-6799

EC2 Instances i-009742ed1bad2478b Connect to instance

## Connect to instance Info

Connect to your instance i-009742ed1bad2478b (user\_instance) using any of these options

EC2 Instance Connect Session Manager **SSH client** EC2 serial console

Instance ID  i-009742ed1bad2478b (user\_instance)

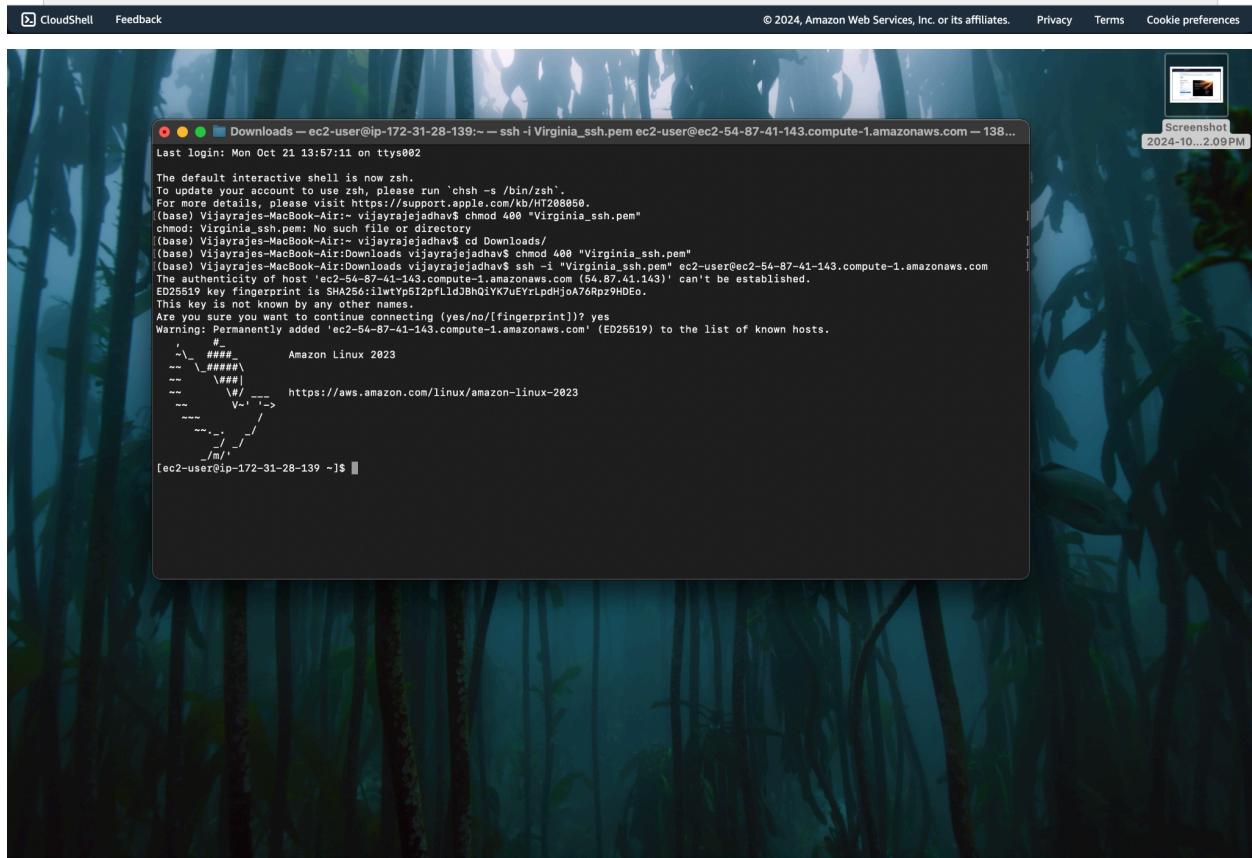
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Virginia\_ssh.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
 chmod 400 "Virginia\_ssh.pem"
4. Connect to your instance using its Public DNS:  
 ec2-54-87-41-143.compute-1.amazonaws.com

Example:

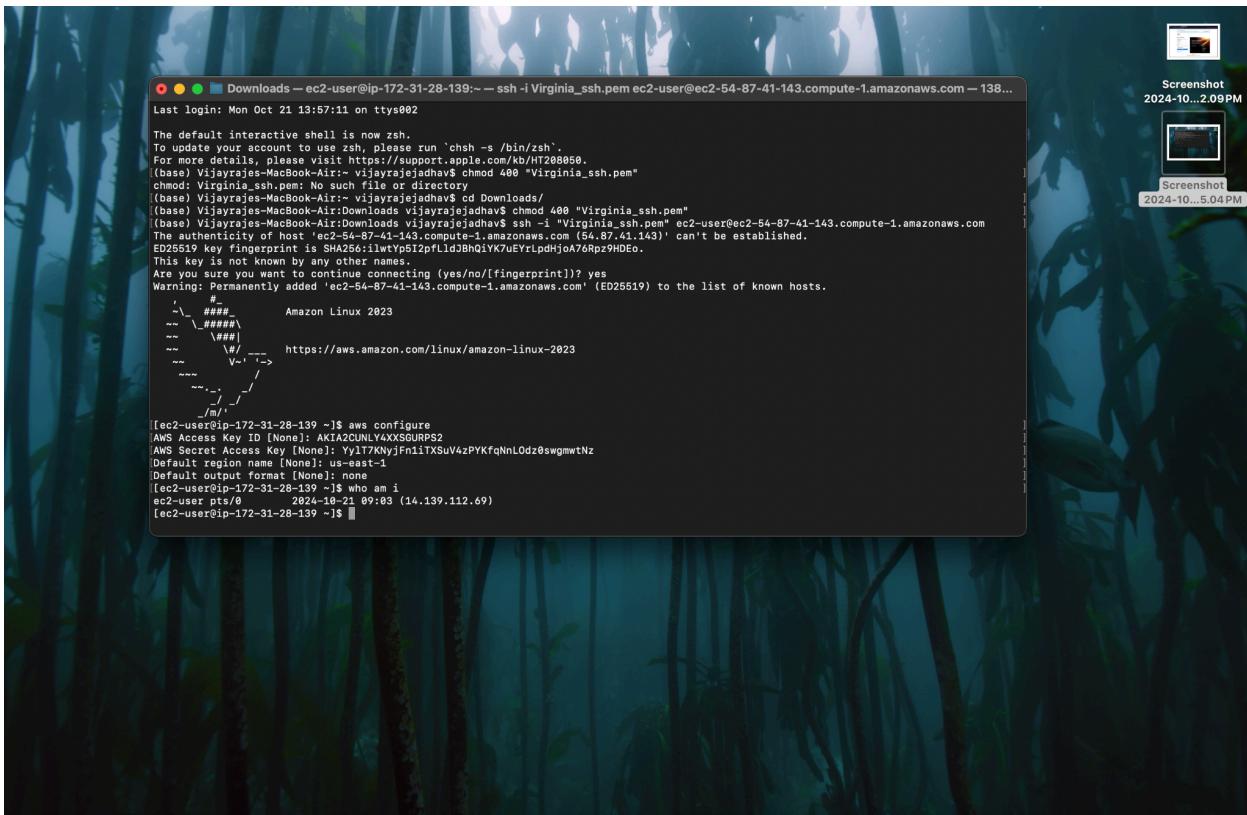
ssh -i "Virginia\_ssh.pem" ec2-user@ec2-54-87-41-143.compute-1.amazonaws.com

**Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

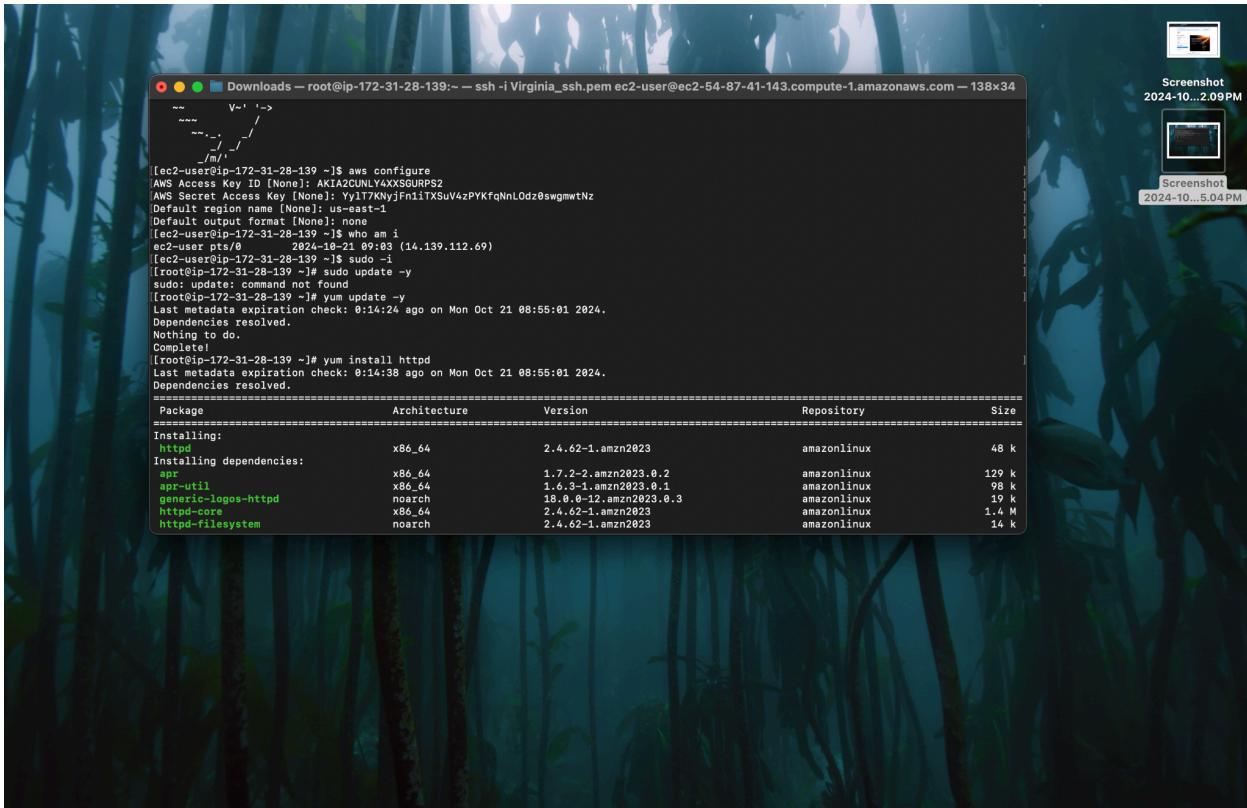
Cancel



## The iam user successfully accessed the ec2 instance with access key



```
○ ○ ○ Downloads — ec2-user@ip-172-31-28-139:~ ssh -i Virginia_ssh.pem ec2-user@ec2-54-87-41-143.compute-1.amazonaws.com — 138...  
Last login: Mon Oct 21 13:57:11 on ttys002  
  
The default interactive shell is now zsh.  
To update your account to use zsh, please run 'chsh -s /bin/zsh'.  
For more details, please visit https://support.apple.com/kb/HT208850.  
(base) Vijayrajes-MacBook-Air:~ vijayrajejadav$ chmod 400 "Virginia_ssh.pem"  
chmod: Virginia_ssh.pem: No such file or directory  
(base) Vijayrajes-MacBook-Air:~ vijayrajejadav$ cd Downloads/  
(base) Vijayrajes-MacBook-Air:~/Downloads vijayrajejadav$ chmod 400 "Virginia_ssh.pem"  
chmod: Virginia_ssh.pem: No such file or directory  
The authenticity of host 'ec2-54-87-41-143.compute-1.amazonaws.com (54.87.41.143)' can't be established.  
ED25519 key fingerprint is SHA256:1lWtvp6I2pfLldJBhQ1YK7uEYrlpdhjoA76Rpz9HDEo.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-54-87-41-143.compute-1.amazonaws.com' (ED25519) to the list of known hosts.  
      #_          Amazon Linux 2023  
~~ \###  
~~ \|##|  
~~ \|#|  
~~ \|/| -- https://aws.amazon.com/linux/amazon-linux-2023  
~~ \|/|  
~~ \|/|  
~~ \|/|  
~~ \|/|  
~~ \|/|  
~/m'/  
[ec2-user@ip-172-31-28-139 ~]$ aws configure  
AWS Access Key ID [None]: AKIA2CUNIYXXSGURPS2  
AWS Secret Access Key [None]: Yj177KnyfNiiTXSuV4zPYkfqNnLOdz0swgmwtNz  
Default region name [None]: us-east-1  
Default output format [None]: none  
[ec2-user@ip-172-31-28-139 ~]$ who am i  
ec2-user pts/0          2024-10-21 09:03 (14.139.112.69)  
[ec2-user@ip-172-31-28-139 ~]$ ■
```



```
○ ○ ○ Downloads — root@ip-172-31-28-139:~ ssh -i Virginia_ssh.pem ec2-user@ec2-54-87-41-143.compute-1.amazonaws.com — 138x34  
      V-  '-->  
~~ \|/|  
~~ \|/|  
~~ \|/|  
~~ \|/|  
~/m'/  
[ec2-user@ip-172-31-28-139 ~]$ aws configure  
AWS Access Key ID [None]: AKIA2CUNIYXXSGURPS2  
AWS Secret Access Key [None]: Yj177KnyfNiiTXSuV4zPYkfqNnLOdz0swgmwtNz  
Default region name [None]: us-east-1  
Default output format [None]: none  
[ec2-user@ip-172-31-28-139 ~]$ who am i  
ec2-user pts/0          2024-10-21 09:03 (14.139.112.69)  
[ec2-user@ip-172-31-28-139 ~]$ sudo -i  
[root@ip-172-31-28-139 ~]# sudo update -y  
sudo: update: command not found  
[root@ip-172-31-28-139 ~]# yum update -y  
Last metadata expiration check: 0:14:38 ago on Mon Oct 21 08:55:01 2024.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@ip-172-31-28-139 ~]# yum install httpd  
Last metadata expiration check: 0:14:38 ago on Mon Oct 21 08:55:01 2024.  
Dependencies resolved.  
=====  
Package           Architecture Version       Repository   Size  
=====  
Installing:  
  httpd            x86_64     2.4.62-1.amzn2023      amazonlinux    48 k  
  Installing dependencies:  
    apr             x86_64     1.7.2-2.amzn2023.0.2  amazonlinux    129 k  
    apr-util        x86_64     1.6.3-1.amzn2023.0.1  amazonlinux    98 k  
    generic-logos-httd noarch    18.0.0-12.amzn2023.0.3  amazonlinux    19 k  
    httpd-core      x86_64     2.4.62-1.amzn2023      amazonlinux    1.4 M  
    httpd-filesystem noarch    2.4.62-1.amzn2023      amazonlinux    14 k  
[root@ip-172-31-28-139 ~]#
```

## Start and install httpd

```

Downloads — root@ip-172-31-28-139:/var/www/html — ssh -i Virginia_ssh.pem ec2-user@ec2-54-87-41-143.compute-1.amazonaws.co...
Installing : httpd-core-2.4.62-1.amzn2023.x86_64
Installing : mod_http2-2.0.27-1.amzn2023.0.3.x86_64
Installing : mod_lua-2.4.62-1.amzn2023.x86_64
Installing : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
Installing : httpd-2.4.62-1.amzn2023.x86_64
Running scriptlet: httpd-2.4.62-1.amzn2023.x86_64
Verifying : apr-1.7.2-2.amzn2023.0.2.x86_64
Verifying : apr-util-1.6.5-1.amzn2023.0.1.x86_64
Verifying : apr-util-openldap-1.6.5-1.amzn2023.0.1.x86_64
Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
Verifying : httpd-2.4.62-1.amzn2023.x86_64
Verifying : httpd-core-2.4.62-1.amzn2023.noarch
Verifying : httpd-filesystem-2.4.62-1.amzn2023.x86_64
Verifying : libbrotli-1.0.9-4.amzn2023.0.2.x86_64
Verifying : mailcap-2.1.49-3.amzn2023.0.3.noarch
Verifying : mod_http2-2.0.27-1.amzn2023.0.3.x86_64
Verifying : mod_lua-2.4.62-1.amzn2023.x86_64
Installed:
apr-1.7.2-2.amzn2023.0.2.x86_64      apr-util-1.6.3-1.amzn2023.0.1.x86_64      apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch  httpd-2.4.62-1.amzn2023.x86_64      httpd-core-2.4.62-1.amzn2023.x86_64
httpd-filesystem-2.4.62-1.amzn2023.noarch  httpd-tools-2.4.62-1.amzn2023.x86_64      libbrotli-1.0.9-4.amzn2023.0.2.x86_64
mailcap-2.1.49-3.amzn2023.0.3.noarch    mod_http2-2.0.27-1.amzn2023.0.3.x86_64      mod_lua-2.4.62-1.amzn2023.x86_64
mod_http2-2.0.27-1.amzn2023.0.3.x86_64
Complete!
[root@ip-172-31-28-139 ~]# systemctl start httpd
[root@ip-172-31-28-139 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-28-139 ~]# cd /var/www/html
[root@ip-172-31-28-139 html]# nano welcome.html
[root@ip-172-31-28-139 html]# ls
welcome.html
[root@ip-172-31-28-139 html]#

```

The webpage can be accessed by instance ip

AWS exam - Google Doc Instances | EC2 | us-east-1 EC2 Instance Connect

us-east-1.console.aws.amazon.com/ec2/home

Instances (1/2) Info Last updated 1 minute ago Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
naya_wala	i-0de10628813f4152c	Running	t3.micro	3/3 checks passed	<a href="#">View alarms</a>	us-east-1d
<b>user_instance</b>	<b>i-009742ed1bad2478b</b>	<b>Running</b>	<b>t3.micro</b>	<b>3/3 checks passed</b>	<a href="#">View alarms</a>	<b>us-east-1d</b>

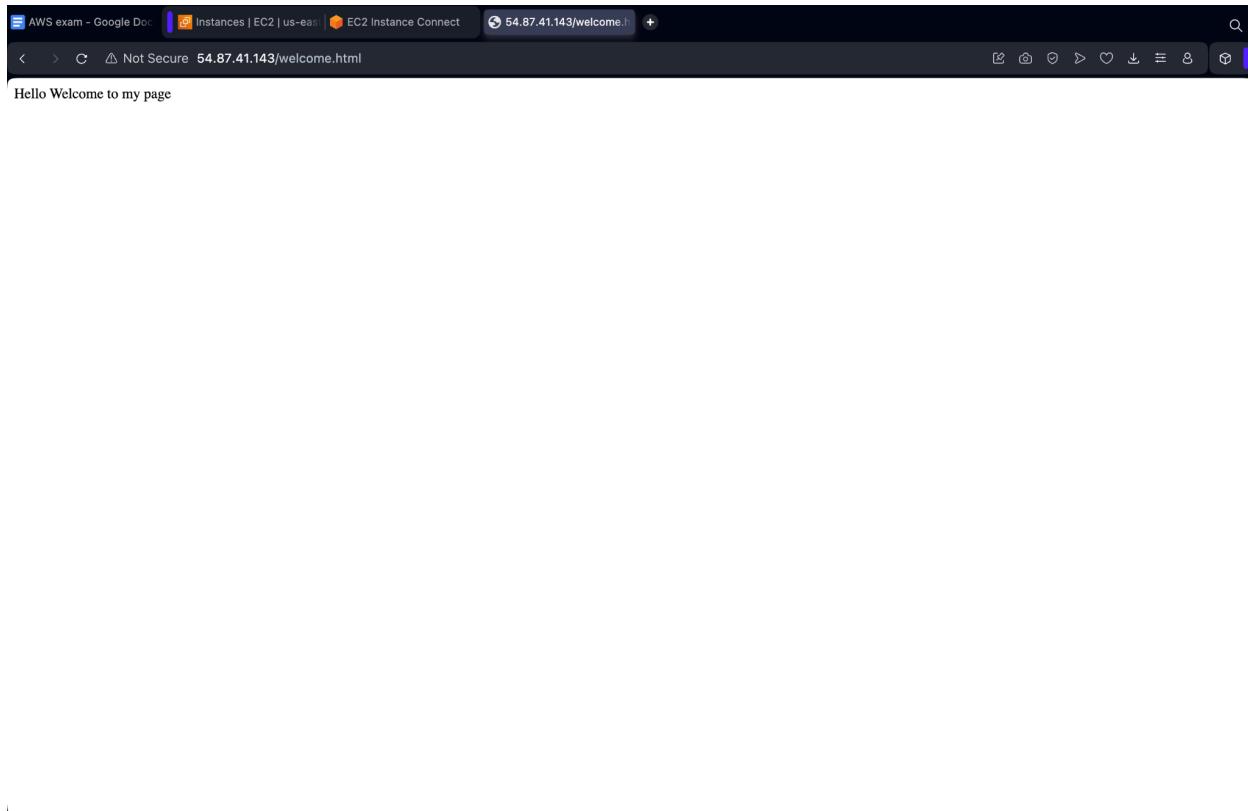
**i-009742ed1bad2478b (user\_instance)**

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info Public IPv4 address copied

Instance ID	i-009742ed1bad2478b (user_instance)	Instance state	Running	Private IP4 addresses	172.31.28.139
IPv4 address	-	Private IP DNS name (IPv4 only)	ip-172-31-28-139.ec2.internal	Public IP4 DNS	ec2-54-87-41-143.compute-1.amazonaws.com   open address
Hostname type	IP name: ip-172-31-28-139.ec2.internal	Instance type	t3.micro	Elastic IP addresses	-
IPV4 (A)		VPC ID	vpc-032188921aaa095d7	AWS Compute Optimizer finding	
Auto-assigned IP address	54.87.41.143 [Public IP]	User: arn:aws:iam::692859946799:user/iam_user is not authorized to perform: compute-optimizer:GetEnroll			

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

A screenshot of the AWS S3 console. The top navigation bar includes links for 'S3 buckets | S3 | us-east-1', 'vpcs | VPC Console', 'Console Home | Console Home | u...', 'Pages', 'IAM policy testing with the IAM pol...', 'IAM Policy Simulator', 'N. Virginia', and 'vijayraje'. The main content area shows the 'Buckets' section. A header for 'Account snapshot - updated every 24 hours' is displayed, along with a 'View Storage Lens dashboard' button. Below this, there are tabs for 'General purpose buckets' (which is selected) and 'Directory buckets'. A table lists two 'General purpose buckets':

Name	AWS Region	IAM Access Analyzer	Creation date
codepipeline-us-east-1-728593405599	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 20, 2024, 23:36:06 (UTC+05:30)
vijayraje	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 20, 2024, 18:36:00 (UTC+05:30)

At the bottom of the page, there are links for 'CloudShell', 'Feedback', '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**⚠️ Turning off block all public access might result in this bucket and the objects within becoming public**

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**Object Ownership [Info](#)**

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.**

**Object Ownership**

**Bucket owner preferred**  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

**Object writer**  
The object writer remains the object owner.

**ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)**

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

S3 buckets | S3 | us-east-1 vpcs | VPC Console Console Home | Console Home | u... Pages IAM policy testing with the IAM pol... IAM Policy Simulator N. Virginia vijayraje

Services Search [Option+S] View details × ⓘ

Successfully created bucket "exampurpose"  
To upload files and folders, or to configure additional bucket settings, choose View details.

Amazon S3 > Buckets

Account snapshot - updated every 24 hours All AWS Regions Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

General purpose buckets Directory buckets

General purpose buckets (3) Info All AWS Regions Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
codepipeline-us-east-1-728593405599	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 20, 2024, 23:36:06 (UTC+05:30)
exampurpose	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 21, 2024, 14:47:21 (UTC+05:30)
vijayraje	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 20, 2024, 18:36:00 (UTC+05:30)

Create bucket

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

vpcs | VPC Console Console Home | Console Home | u... Pages IAM policy testing with the IAM pol... IAM Policy Simulator N. Virginia vijayraje

Services Search [Option+S]

Edit access control list (ACL) Info

Access control list (ACL)  
Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Canonical ID: 6161515c045484b0391792 ed69f8937a677a6e87e6f7d8b2 fc69a6d704a35419		
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> List <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> List <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input type="checkbox"/> List <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers		
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> List <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.  
[Learn more](#)  I understand the effects of these changes on my objects and buckets.

Access for other AWS accounts  
No other AWS accounts associated with the resource.

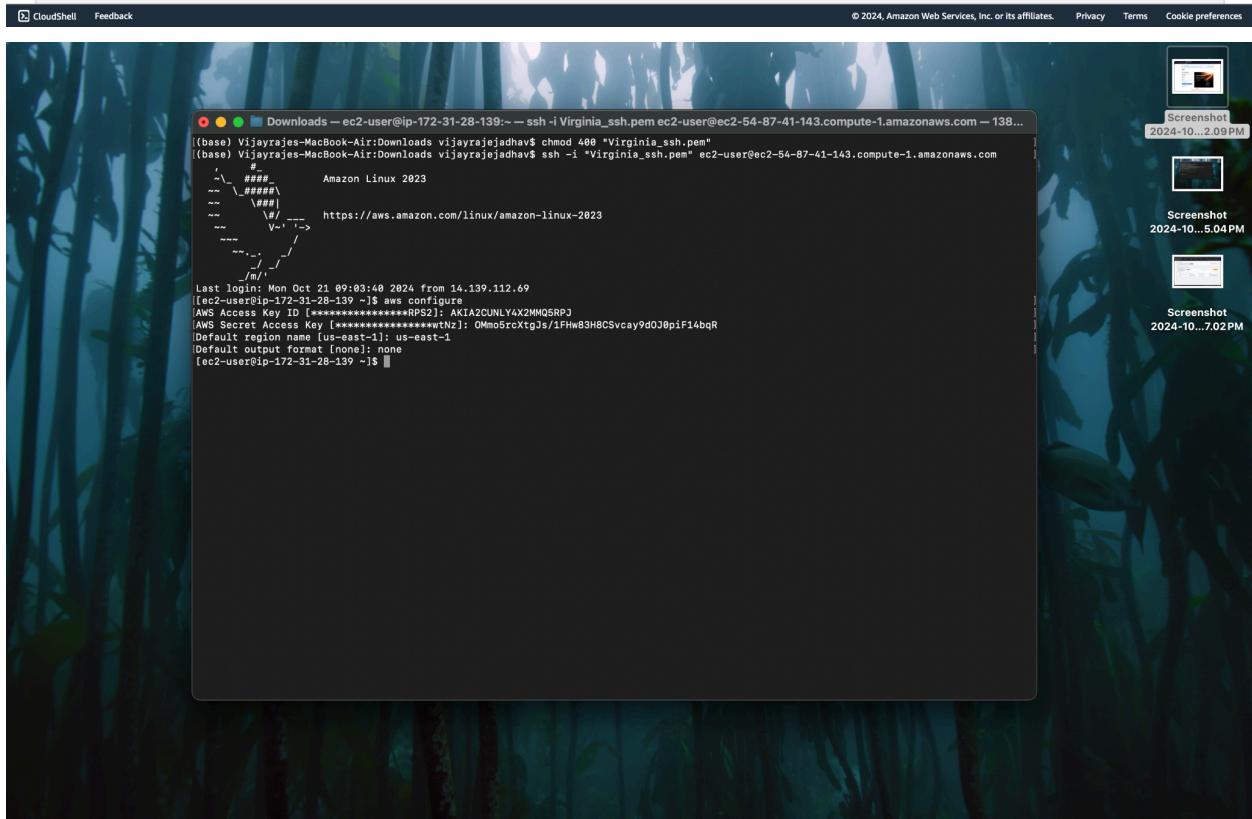
Add grantee

Cancel Save changes

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

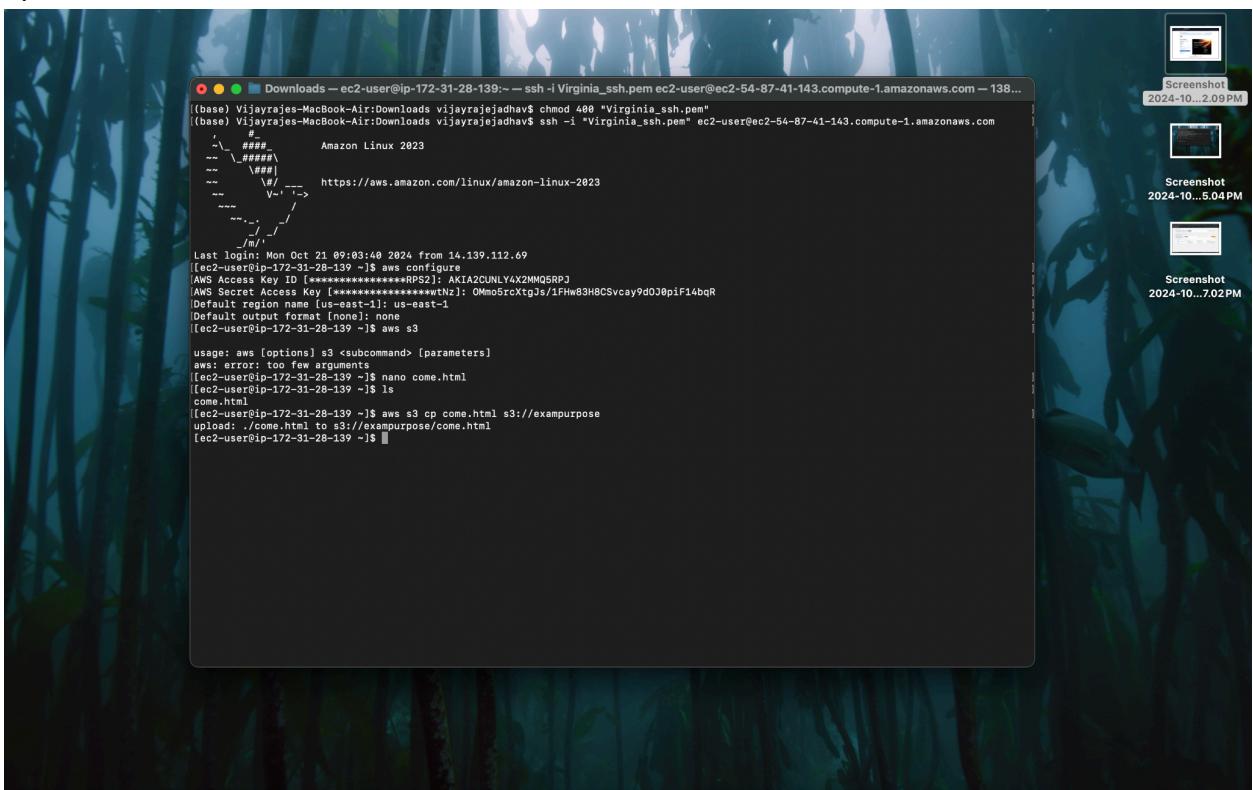
## Create access key for root user

The screenshot shows the 'Create access key' wizard in the AWS IAM console. The title bar says 'Create access key | IAM | Global'. The main content area is titled 'Alternatives to root user access keys' with a note: 'Root user access keys are not recommended'. It advises against creating root access keys because you can't specify the root user in a permissions policy. Instead, it suggests using IAM roles or IAM Identity Center for temporary credentials. A checkbox at the bottom states: 'I understand creating a root access key is not a best practice, but I still want to create one.' A 'Create access key' button is visible.



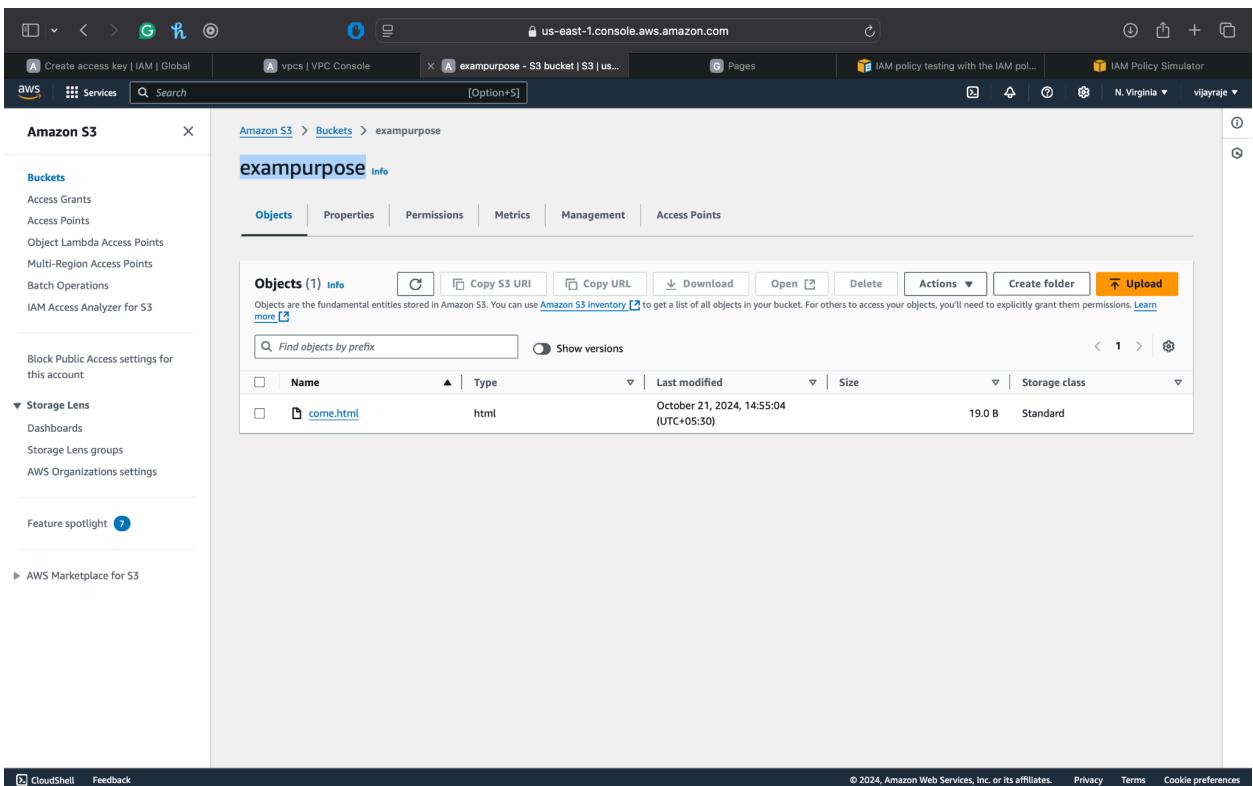
Get access through root id in instance

## Upload the html file to the bucket



```
(base) Vijayrajes-MacBook-Air:Downloads vijayrajejadav$ chmod 400 "Virginia_ssh.pem"
(base) Vijayrajes-MacBook-Air:Downloads vijayrajejadav$ ssh -i "Virginia_ssh.pem" ec2-user@ec2-54-87-41-143.compute-1.amazonaws.com
Last login: Mon Oct 21 09:03:40 2024 from 14.139.112.69
[ec2-user@ip-172-31-28-139 ~]$ aws configure
AWS Access Key ID [*****]: AKIAZUNLYAX2MMQ5RPJ
AWS Secret Access Key [*****]: OMmo5rcXtgJs1FHw8HBCSvca9dOJ0piF14bqR
Default region name [us-east-1]: us-east-1
Default output format [none]: none
[ec2-user@ip-172-31-28-139 ~]$ aws s3 cp come.html s3://exampurpose
upload: ./come.html to s3://exampurpose/come.html
[ec2-user@ip-172-31-28-139 ~]$
```

check the file in the bucket



The screenshot shows the AWS S3 console interface. The left sidebar is collapsed, and the main area displays the 'exampurpose' bucket. The 'Objects' tab is selected, showing one object named 'come.html'. The object details are as follows:

Name	Type	Last modified	Size	Storage class
come.html	html	October 21, 2024, 14:55:04 (UTC+05:30)	19.0 B	Standard

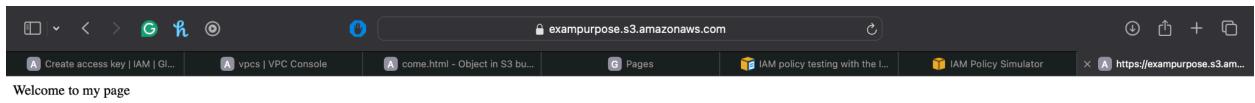
## Make it public acl

The screenshot shows the 'Amazon S3 > Buckets > exampurpose > Make public' interface. A warning message states: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below this is a 'Specified objects' section showing a single file: 'come.html' (Type: html, Last modified: October 21, 2024, 14:55:04 (UTC+05:30), Size: 19.0 B). At the bottom right is a prominent orange 'Make public' button.

Now copy the object url and check

The screenshot shows the 'Amazon S3 > Buckets > exampurpose > come.html' object details page. The object name is 'come.html'. In the top right, there are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. The 'Properties' tab is selected. Under 'Object overview', the object's properties are listed: Owner (vijayraje1137), AWS Region (US East (N. Virginia) us-east-1), Last modified (October 21, 2024, 14:55:04 (UTC+05:30)), Size (19.0 B), Type (html), and Key (come.html). To the right, the S3 URI is listed as 's3://exampurpose/come.html'. Under 'Object management overview', it says 'The following bucket properties and object management configurations impact the behavior of this object.' Under 'Bucket properties', 'Bucket Versioning' is mentioned with a note: 'When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.' Under 'Management configurations', 'Replication status' is listed with a note: 'When a replication rule is applied to an object the replication status indicates the progress of the operation.'

It is working



<https://exampurpose.s3.amazonaws.com/come.html>

Url of that bucket